Minimizing Packet Drop Due to Black Hole Attack in Wireless Ad-Hoc Network Using Intrusion Detection System

Constance Nneka Eze[1], Chikani N.I[2], Nnaji B.Ugochukwu[3]

[1]Department of Computer Engineering Enugu State Polytechnic Iwollo Enugu, Nigeria

[2]Department of Electrical and Electronic Engineering Enugu State Polytechnic Iwollo Enugu, Nigeria

Abstract: **A black hole attack is a place in computer networking whereby incoming and outgoing traffic are silently discarded or dropped without notifying the source that the data sent was unable to reach its destination. A highly successfully black hole attack can prevent all data from reaching its destination and are undetectable. This attack is a significant threat to any wireless Ad-hoc Network because it causes isolation in the Network and does that untraced. The aim of this research work focus on minimizing black hole attack in wireless Ad-hoc Network. To do this, the effect of black hole attack on wireless Ad-hoc Network in terms of packet delivery ratio was first determined. This was done by comparing the packet delivery ratio when intrusion detection system was activated and when it was not activated. Next was to reduce the rate of packet loss as a result of black hole attack this was achieved by generating a packet transmission scheme, which will enable the nodes to gain authentication in the network before packets will be sent to them, thereby reducing the rate of packet loss. After this an intrusion detection system was implemented in all the node. Then a sequence number model and Wi-Fi mini point adapter method was used in modeling intrusion detection system and the corresponding throughput was achieved by calculating the amount of data transferred from source to destination in a given amount of time. All the above work was performed by simulation using PHP-MYSQL and MATLAB. The results obtained showed that the packet loss in ad-hoc wireless network under attack was reduced by 1% when compared by the work done by other researchers.**

I. INTRODUCTION

Nowadays, there is an increasing interest on research focused on the provision of proposals for securing ad hoc routing protocols against black hole attack. A highly successful Black Hole attack can prevent all data from reaching its destination and are undetectable. Therefore, this attack is a significant threat to any wireless ad hoc network because it causes isolation in the network and does that untraced.

Researchers have proposed various techniques to minimize black hole attack in wireless ad-hoc networks. Recent efforts are directed towards the use of multiple RREP (Route Reply) and IDS (Intrusion Detection System) approaches. The IDS approach can cooperatively isolate the malicious node, but has failed to deal with collaborative black hole attack, while the RREP approach have a major drawback of adding network delay. So far, there is no perfect technique to prevent black hole attack in wireless ad-hoc networks.

New researchers are adopting already existing techniques and aiming at improving on this techniques. The results are a better modified technique that has less of the weaknesses of the predecessor. This is the motivation for this research work which would attempt to adopt the IDS approach and enhance its ability in minimizing the black hole attack. Black hole attacks cause total loss of Network packets. The problems associated with packet drop can be severe and irrespirable, sensitive information or signals needed in operations when lost could mean the failure of such operations. The need to secure wireless ad-hoc network against this attack becomes as important as achieving success.

A security threat like black hole could be very adverse to the activities of the military, rescue agencies, corporate bodies and any organization that employs the Wireless Ad hoc Network for communication and transfer of information. Also, for Network Administrators and professionals, packet drop due to black hole attack is a security challenge of significant consideration.

Wireless ad hoc Network suffers black hole attack due to the lack of security features of the on-demand protocols, such as AODV (Ad-hoc On Demand Distance Vector). This research seeks to propose a technique for securing the on-demand protocol, AODV, thereby minimizing packet drop due to black hole attack on Wireless ad-hoc Network.

The aim of this research work is to minimize black hole attack in Wireless Ad-hoc Network. This aim will be achieved in the following objectives:

i. To determine the effect of Black Hole Attacks on the wireless ad hoc network in terms of packet delivery ratio.
ii. To reduce the rate of packet loss as a result of black hole attack
iii. To model an intrusion detection system (IDS) approach to detect and minimize the black hole attack and improve throughput.
iv. To simulate the above using php-Mysql and MATLAB.

II. MATERIALS

Wireless ad-hoc network comprises of the following equipment's

- Wireless router
- Stations
- Packet tracer simulation tool
- Network switch
- Modem
- MATLAB
- Php-MYSQL
- Laptop Computer
- Intrusion Detection System Software etc.

2.1 Equations

i. Forwarding Packet Ratio: Is the relaying of packets from one network segment to another by nodes in a computer network.

Forwarding Packet Ratio = $\underline{F [F, h] = R [F, h+1)}$(1) 1)

ii. Packet Delivery Ratio: It is the ratio of the packets that are successfully delivered to the destination.

$$\text{Packet delivery ratio} = \frac{\text{Number of Packets Received}}{\text{Number of Packets sent}}$$

$$= \text{destination} \frac{R(F,h)}{R(F,0)} < R^{thres\ (F)} \text{.....(3)}$$

iii. Packet Loss: The total number of packets dropped during the simulation

Packet Loss = Total Number of Dropped Packet Total Number of Sent

iv. Throughput: It is the amount of data transferred over the period of time expressed in bits per second.

Throughput (bit) =N$\underline{\text{umber of Delivered Packet X Packet}}$

Size X 8 Simulation Time.

III. METHODOLOGY

The research work proposed to minimize packet drop due to black-hole attack in wireless Ad-hoc Network using Intrusion Detection System (IDS) with Anti-black hole mechanism. The project was carried out in a simulation environment. This was done with PHP-MYSQL and MATLAB. To detect the malicious node in the network .virtual Wi-Fi mini point adapter was used, Virtual Wi-Fi miniport adapter is one of the verification technique, all nodes have a legitimate Digital Signature. Then the above mention objective was implemented as follows: *The determination of the effect of black hole attack on wireless ad-hoc network in terms of packet delivery ratio*

This was done by carrying out a black hole attack, when the malicious node receives an route request (REEQ) message, without checking it routing table, immediately send a false route reply (RREP) messages giving a route to destination over itself, here the malicious node attacks all route request messages this way and takes over all routes in that case all packet sent at this point are not to be found due to black hole attack.

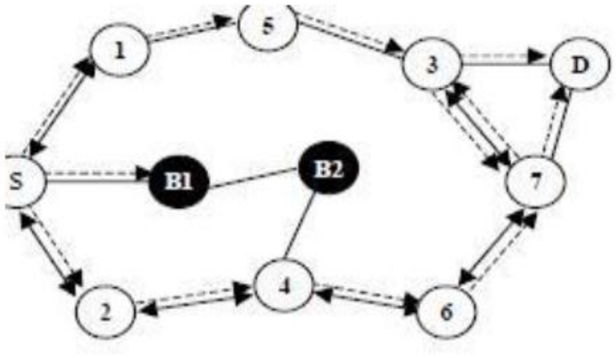


Fig 1: Black hole attack

From the diagram we assume that node B_1 and B_2 are the malicious node (Black hole node) where S is the source and D is the destination were node S as the sender node broadcast the route request packet to all radio range nearest neighbor, remember that node B_1 and B_2 are the malicious node certainly responded route reply packet to sender node S sends data packet that was supposed to go to node 7 but in the middle of transmission node B_1 and B_2 captured all the data packet and cannot send Transmission control protocol Acknowledgement to the sender node so that transmission control protocol has a malicious node.

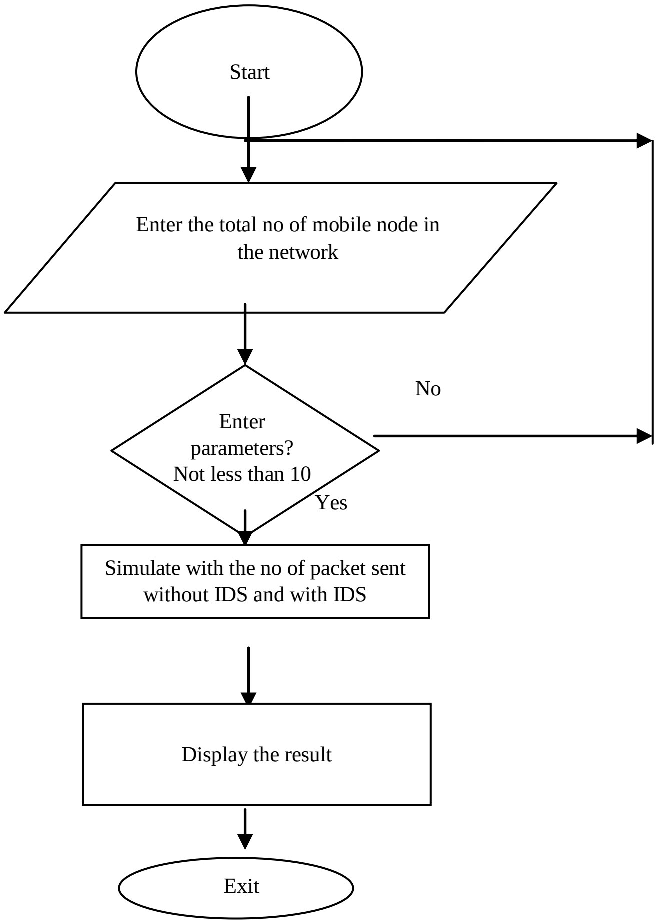

Start
Enter the total no of mobile node in the network
Enter parameters? Not less than 10
No
Yes
Simulate with the no of packet sent without IDS and with IDS
Display the result
Exit

fig 2. Flow chart for the determination of the effect of black hole attack on the wireless ad-hoc network in terms of packet delivery ratio.

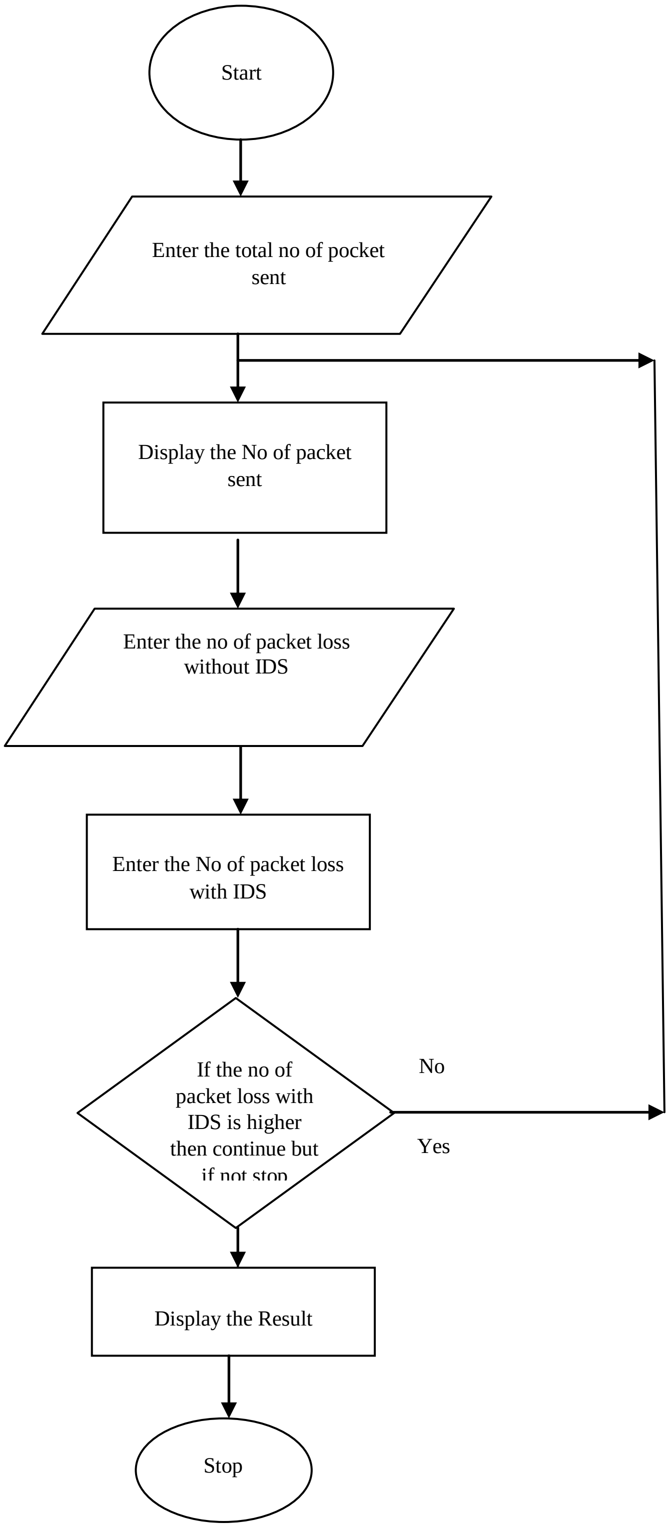

Start
Enter the total no of pocket sent
Display the No of packet sent
Enter the no of packet loss without IDS
Enter the No of packet loss with IDS
If the no of packet loss with IDS is higher then continue but if not stop
No
Yes
Display the Result
Stop

Fig 3. A flow chart that shows how the rate of packet loss as a result of black hole attack was achieved

This was performed by configuring two nodes to behave as a malicious node that is packet drop which was cause by black hole attack. This black hole is a situation where by an internet protocol (IP) address in which no address has been assigned to this two nodes are been refers to as dead IP address which makes it undetectable.

Modeling an intrusion detection system (IDS) approach to detect and minimize the black hole attack and improve throughput.

This was achieved by implementing intrusion detection in all the nodes to determine the ten different sizes of packets and corresponding throughput.

Research Design

The proposed(IDS) scheme to solve black hole attacks in wireless Ad-hoc network plants an anti-black hole mechanism (ABM) in all network nodes. The ABM employs an additional tables which the contents including the source and destination ID, source sequence number, maximum hop count value, broadcasting node ID, Digital Signature and expiration time. The research also focused on identifying the secure path for transmission using Digital Signature. Each node was assigned a Digital Signature. Authentication mechanism was used to compare the host id, ip-address, and Digital Signature of interacting nodes. The result shows that when the ID on a node match a previously stored ID, the node is a valid path, otherwise it is an invalid path. but the Digital Signature used here was for co-operative black hole attack .The research extended to detecting Cooperative Black hole which is when the malicious nodes are acting in a group.

The Experimental

The algorithm for the proposed intrusion detection system in a wireless Ad-hoc network is as follows:

Algo (Blackhole_attack_detection)

Input: no. of nodes n, Source node, Destination Node, digital signature;

Output: Detection and prevention of Black hole Attack, Find the Best Path for routing; Begin Create the network for the input node (of n number nodes) Define Source node & Destination Node Find the neighbors node of source node. For source to destination Send Route Request to neighbor nodes for finding the destination If next node is destination Then direct path is established Else Broadcast the RREQ to next neighbors End for destination to source Select the path with average hop counts Unicast RREP to pervious node with Digital Signature Verify If (all Signature are legal) Establish a path for data transfer. If (Any intermediate or destination node is malicious node) Then add the malicious node information in malicious node column and again rebroadcast Route request (RREQ) End for End. **Data Source:** The program designed involved some input forms in order to achieve or derived some required outputs. This form relates to packet transmission in wireless ad – hoc network. Fig 4. Shows the process of detecting black hole attack in wireless ad hoc network

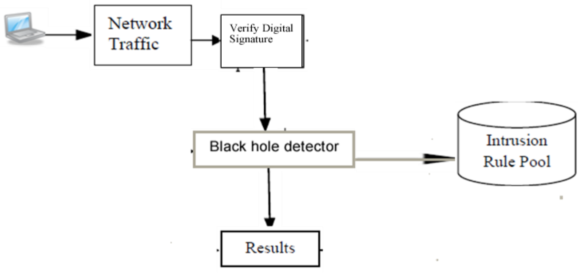
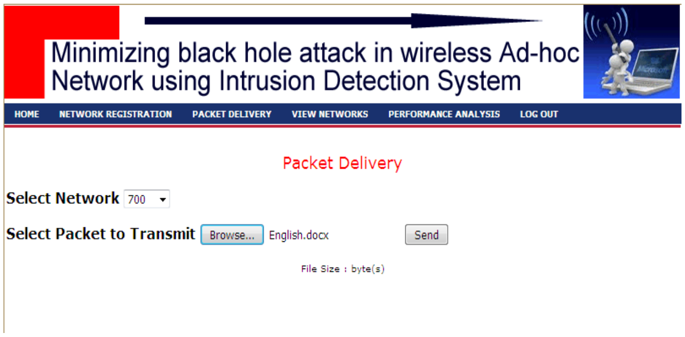


Fig 4: Detecting black hole attack in wireless ad hoc network

As shown in Figure 4, the network traffic is generated from the source node destination node. Profiled information are involved in everyday packet transfer, therefore, the security of systems must be maintained.

In other cases, packets are transmitted through intermediate nodes and involve more complex routing and packet delivery authentication. Below are some of the interfaces simulated for detecting black hole attack in wireless ad-hoc network.



Minimizing black hole attack in wireless Ad-hoc Network using Intrusion Detection System

Packet Delivery

Select Network 700

Select Packet to Transmit English.docx

File Size : byte(s)

Fig 5: packet transmission source node.

Fig 5 shows the implemented interface for originating packet delivery. The user selects the packet to transmit to the destination. The interface captures the packet size, the source node, the IP address and SSID. the system was implemented without integrating intrusion detection system for detecting co-operative black hole attack. When the packet was transmitted, majority of the packets transmitted was not delivered as a result of co-operative black hole attack. Figure 6 shows a diagram dipicting how the packet transmitted from the source node ended up in the black hole attack thereby not reaching the desitnation.

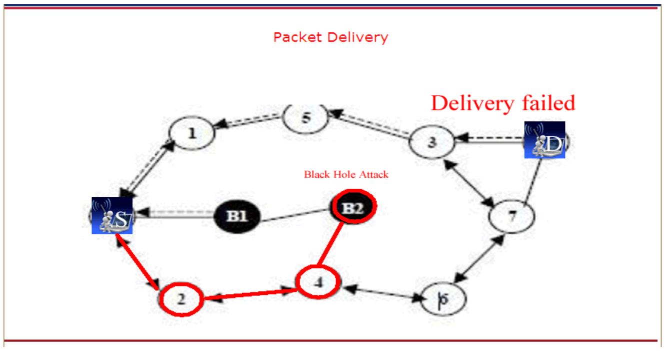


Fig 6: Packet delivery failed as a result of co-operative black hole attack

The figure 6 shows the node S is source node and node D is the destinations node. The node S broadcast the route request within communication range. The node 1 receive the route request (RREQ) packet and forward to the next node 5 which in turn forwarded it to node 3 from where the packet was forwarded to the destination. This process is going on until the packet reaches the destination node.

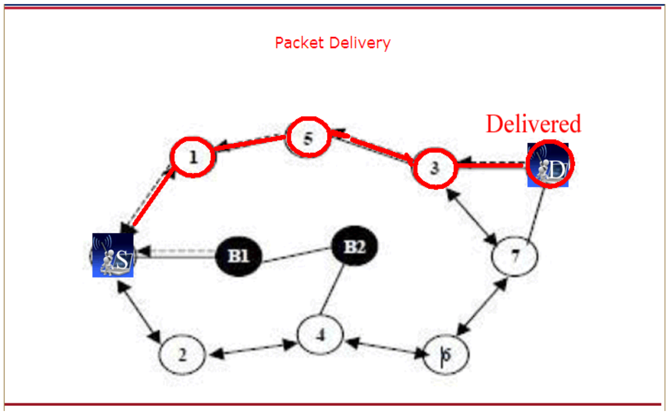


Fig 7: Packet delivery successful as a result of implementation of intrusion detection system Figure 7 shows that the packet was successfully delivered as a result of the intrusion detection system. All co-operative black hole attack was detected and avoided.

IV. RESULTS AND DISCUSSION

Table 1: **Simulated data from the packet delivery time from Afrihub IMT**

Packet Size (KB)	Delivery Time(Seconds)	
	Without IDS	With IDS
21	4	1
36	6	3
46	8	5
60	11	6
70	13	7
137	26	14
159	30	16
166	31	17
191	36	19
232	44	24

The table 1. Shows the simulated data from the packet delivery time, and the ten different sizes of packets and the corresponding delivery time in seconds with and without intrusion detection system (IDS). results obtained from running the simulation program using different data load. In figure 8. it is observed that the higher the size of packet, the more time required completing the packet delivery to its destination. This was performed by simulating the packet delivery time without intrusion detection system, which shows that the time it took packets to reach its destination was been measured with the system time and the graph was plotted against packet delivery time (seconds) verses packet size kilobyte (Kb).

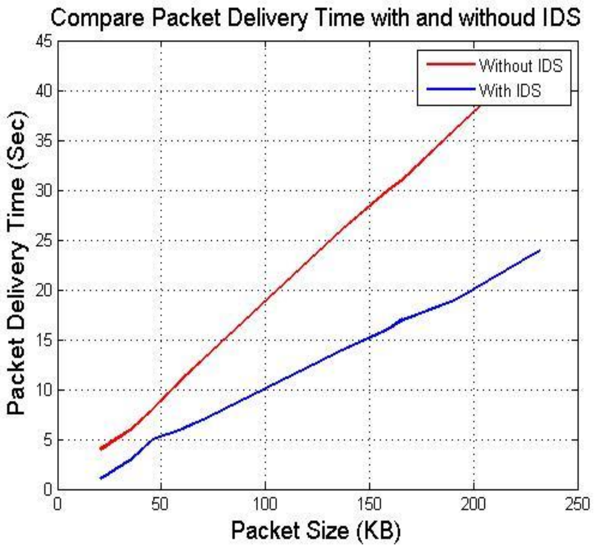


Fig 8: The Comparison of the two different techniques

In figure 8, it is observed that by comparing the performance of two different techniques which is the packet delivery time with intrusion detection system and the packet delivery without intrusion detection system (IDS) it is observed that the simulation results obtained by running the two compared modes, different load have been used to determine the processing power and performance of the compared algorithms shows that the system with intrusion detection system delivers packets faster than the one without intrusion detection system.

Table 2: Number of Packets Delivered

No of Packet Sent	No of Packet Received Without IDS	No of Packets Received with IDS
20	8	19

The table 2 represents the packets sent and packet received for the twenty different sizes of files.

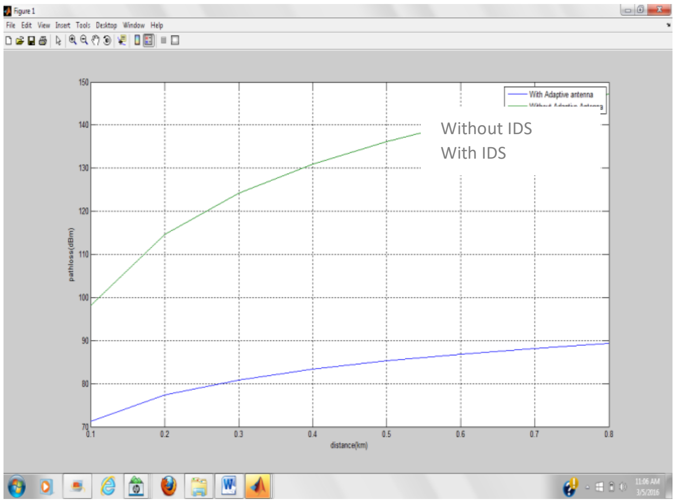


Fig 9: The graph that shows the total packet received, total packet sent, total packet received without (IDS) total packet received with (IDS)

Fig 9, comparing the number of packet delivered. This was done by comparing packet received, total packet sent, total packet received without intrusion detection system and total packet received with intrusion detection system also the packet sent and packet received for the twenty different sizes of files after the simulation the results showed that the number of packets received was very high and close to the no of packets sent when intrusion detection system was implemented but low when intrusion detection system was not implemented.

Table 3: Packet Delivery Ratio

No of Packet Sent	No of Packet Received Without IDS	No of Packets Received with IDS
1.0000	0.4000	0.9500

The table 3 represents the packets delivery ratio which is packet received / packet sent.

In fig 9, it represent the packets delivery ratio which is packet received/packet sent, the comparison for packets delivery ratio with and without intrusion detection system. detection system (IDS) was not implemented.

Table 4: Packet Loss

No of Packet Sent	No of Packet Loss Without IDS	No of Packets Loss with IDS
20	12	1

The table 4. represents the packets loss which is Number of packet send – Number of packet received.

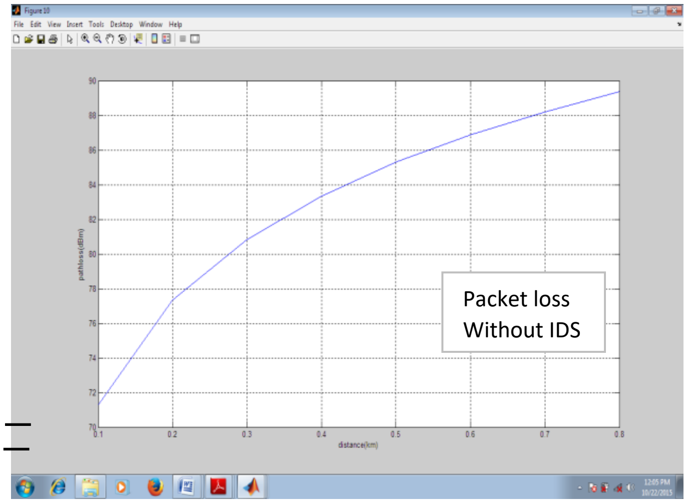


Fig 10: The graph that shows the packet loss without IDS.

In fig 10, represents the packets loss in which the number of packet send-number of packet received and the comparison for total packet loss with and without intrusion detection system (IDS) it showed that the number of packets loss was very high when intrusion detection system was not implemented but low when intrusion detection system was implemented

Table 5: Throughput

Packet Size (KB)	Throughput Without IDS	Throughput With IDS
21	5.13	10.26
36	6.00	12.00
46	5.74	11.48
60	5.44	9.98
70	5.35	9.94
137	5.28	9.81
159	5.30	9.93
166	5.37	9.79
191	5.32	10.07
232	5.28	9.68

The table 5 represents the ten different sizes of packets and corresponding Throughput. In fig 11, represents the ten different sizes of packets and corresponding throughput, to do is packet delivery throughput with changes in packets size kilobyte (kb) without intrusion detection system and packet delivery throughput without changes in packet size kilobyte (kb) this graph was achieved by simulating the packet delivery throughput without intrusion detection system. In fig 11, represents the ten different sizes of packets and corresponding throughput, to do is packet delivery throughput with changes in packets size kilobyte (kb) with intrusion detection system and packet delivery throughput with changes in packet size kilobyte (kb) this graph was achieved by simulating the throughput verses packet size (kb) kilobyte per second.

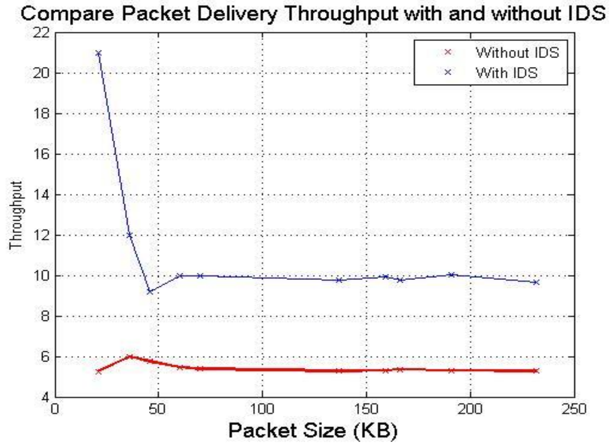


Fig 11: Throughput Comparison with and without IDS

Fig 11, showed the simulation throughput obtained by running the two different packet transmission modes. Different load have been used to determine the processing power and throughput of the compared algorithms. Fig 11 shows that a higher throughput was achieved with intrusion detection system (IDS), while a lower throughput was gotten without intrusion detection system.

REFERENCE:

[1] Deepail,R.,&Kapil, H.(2014) Detection and Prevention of gray hole and black hole attack in MANET: International Journal of Computers and Technology, 13,50305038.

[2] Gagandeep, Aashima, & Pawan, K. (2012). Analysis of Different Security Attacks in MANETS on Protocol Stack A-Review. International Journal of Engineering and Advanced Technology (IJEAT), 1, 269 – 275.

[3] Gurjar, A.A., & Dande, A.A. (2013). Black Hole Attack in MANETs: A Review Study. International Journal of IT, Engineering and Applied Sciences Research (IJIEASR), 2(3), 12-14.

[4] Hicham, Z., Ahmed, T., Rachid, L., & Noureddine, I. (2013). Mitigating Black Hole attack in MANET by Extending Network Knowledge. International Journal of Advanced Computer Science and Applications (IJACSA),4. 152 – 158.

[5] Wikipedia the free encyclopedia, (2016) Overview of wireless Ad-hoc Network. Mitigating Routing Misbehavior in Ad Hoc Networks'', Proc. 6th Annual International conference. Mobile Comp. and Net., Boston, MA. PP. 255 – 265. August 2000.51.

[6] Shikha (2014) Impersonation attack.. ''An Intrusion Detection Tool for AODV-BASED AD-HOC WIRELESS NETWORKs'', Proc. Of the 20th Annual Computer Security Applications Conference (ACSAC'